Procedure No. 5-08A

REVIEW OF COMPUTER SYTEMS

Background

Government Auditing Standards require auditors to obtain sufficient, competent, and relevant evidence that computer-processed data are valid and reliable when those data are significant to the auditors' findings. This work is necessary regardless of whether the data are provided to auditors or auditors independently extract them. Auditors should determine if other auditors have worked to establish the effectiveness of the controls over the system to ensure that it produces valid and reliable data. If they have, auditors may be able to use that work. If not, auditors may determine the validity and reliability of computer-processed data by direct tests of the data. Auditors can reduce the direct tests of the data if they test the effectiveness of general and application controls over computer-processed data, and these tests support the conclusion that the controls are effective.

List of Threats and Controls

The following are threats (*T*) and controls (C) pertaining to computer-based systems. The auditor should confer with the auditee to determine whether there are other threats that should be included in this list and whether the listed controls and any alternate or additional controls are documented and in place. In testing the effectiveness of general and application controls, the auditor should determine whether the controls the auditee has implemented adequately mitigate the threats.

T1. The computer system does not meet the needs of the City.

- C1. Establish written objectives and policies for the computer application approved by senior management.
- C2. Document the system features and the related objectives met by each feature.

T2. Important activities and functions in maintaining the computer systems are not performed.

- C3. Document general and application control procedures.
- C4. Provide adequate training and supervision to all personnel responsible for performing control procedures.
- C5. Prepare written statements of responsibilities, which assign responsibility for specific activities and functions.
- C6. Prepare a written maintenance schedule.
- C7. Require a documented supervisory review to ascertain that specific activities and functions are performed as scheduled.

T3. The computer system is unable to recover after a disaster or computer failure.

- C8. Prepare a backup and recovery plan including periodic testing of the plan.
- C9. Provide offsite storage of backup files.
- C10. Conduct tests to reconstruct systems and databases from data held in off-site storage.
- C11. Require a documented supervisory review to ascertain that periodic testing of the backup and recovery plan is performed.

Unauthorized changes in the computer systems are made.

C12. Require that appropriate written authorization be obtained before a change is initiated.
C13. Require that all changes be supported by a standard request form that describes the nature of and reason for the change.
C14. Implement software and physical measures to prevent and detect unauthorized changes to systems software and applications.
C15. Require a documented supervisory review to ascertain that only authorized changes are implemented and that implemented changes are promptly reflected in revised written procedures.

T4. Information processing problems are not timely detected or corrected.

C16. Maintain a record of all problems and the follow-up actions taken.
C17. Maintain a record of manufacturers' warranties and ascertain that all repairs that are within the warranty period are performed under the warranty.
C18. Require a documented supervisory review to ascertain that information processing problems are promptly resolved.

T5. Computer equipment is lost or not properly cared for.

C19. Maintain an inventory of computer equipment, including computer units, terminals, printers, and input devices.
C20. Affix permanent City labels on all computer equipment.
C21. Assign responsibility for each piece of computer equipment to a specific employee.
C22. Perform an annual physical inventory of computer equipment and prepare a written report of the inventory, including an investigation of any lost or damaged equipment.

T6. Unauthorized or erroneous transactions are processed.

C23. Establish written procedures to ensure that only authorized and correct transactions are processed.
C24. Incorporate input checks in the system.
C25. Require a written independent review to ascertain that input procedures and checks are functioning properly and consistently.

T7. Not all authorized transactions are processed.

C26. Number transactions, check the numeric sequence, and investigate the reasons for missing numbers.
C27. Establish control totals and use the control totals to check the completeness of processing.
C28. Require a written independent review to ascertain that number sequence integrity and control totals are in place and used to check the completeness of processing.
C29. File each record in a significant and planned sequence to facilitate retrieval during a subsequent review.

T8. Output is incomplete, inaccurate, or inconsistent.

C30. Provide the software capability to scrutinize and analyze data.
C31. Incorporate control totals in report summaries.
C32. Agree summary records to the supporting detailed records.
C33. Check the consistency of multiple versions of data.
C34. Check report consistency from period to period.

T9. Unauthorized individuals tamper with sensitive data and program files.

C35. Identify sensitive data files and programs and protect them to an appropriate level of security.
C36. Establish standards to control the use of passwords.
C37. Restrict access to supervisory and utility programs.
C38. Lock computer terminals and other computer equipment or keep them in secure areas.
C39. When information systems processing is carried out at multiple sites with extensive use of telecommunications, use specific and appropriate security techniques.
C40. Ascertain that software licenses are valid and no pirated software is being used.